Information Commissioner's Office

Draft data protection and journalism code of practice

ico.
Information Commissioner's Office

Contents

About this code

At a glance

- This code contains practical guidance for organisations and people using personal data for journalism under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).
- Personal data is any information about a living and identifiable person, that is, or will be, stored on a digital device or kept in an organised way.
- This code is mainly for media organisations and journalists.
- It will help you to comply with your legal obligations and follow good practice.
- You **must** balance freedom of expression with other fundamental rights in a democratic society, such as data protection, which is part of the broader right to privacy.
- This code is about data protection. It does not concern press conduct or standards in general, which are covered by industry codes. However, it may help you comply with industry codes and other privacy laws.
- This code is a statutory code of practice under the DPA 2018.
- The Information Commissioner's Office (ICO), courts and tribunals must take this code into account, where relevant.
- The ICO must review how personal data is used for journalism. This code will help us to consider this. We must also keep the code itself under review.

In more detail

Who is this code for?

This code contains practical guidance for organisations and people using personal data for journalism under the UK GDPR and the DPA 2018. We may refer to this in the code as data protection law.

What does using personal data mean?

Personal data **is** any information:

- about an identifiable living person; and
- that is, or will be, stored on a computer or other digital device, or in an organised way.

It does not need to be private. Anything about a person can be personal data – even information that is public knowledge or about someone's professional life. For example, a job title.

Personal data does not need to be factual. For example, opinions about a person can be personal data.

Information is **not** personal data if it is:

- a paper record that you do not plan to put on a digital device or organised file (eg handwritten notebooks);
- information about a deceased person; or
- truly anonymous – if you can still identify someone from the details or by combining it with other information, it is personal data.

In the code, we refer to "using" personal data, which means the same as "processing" personal data. Processing is the legal description used in data protection law. Using personal data means anything that you do with it, including collecting, recording, storing, publishing, sharing or deleting it.

This code applies to organisations using personal data that operate within the UK. It also applies to organisations outside the UK that offer goods or services to people in the UK.

The code is mainly for media organisations and journalists, such as the press, broadcast media and online news outlets. This includes press agencies and freelance journalists providing stories to media organisations.

When we say 'you' in the code, we are mainly addressing the person with the main legal responsibility for complying with data protection law (eg the head of the media organisation). However, in practice, various people within an organisation have some data protection responsibilities, so this code will help anyone using personal data for journalism, including journalists.

We also recognise that journalism is not limited to media organisations or the journalists they employ. So the code also applies more broadly to other groups and people, including campaign groups or members of the public using personal data for journalism.

How will this code help us?

This code will help you to understand important parts of data protection law and think about how to apply it in practical ways. It focuses on seven key principles, which are largely flexible and based on risk. It says that you **must**:

1. take steps to protect personal data;
2. keep it secure;
3. use it lawfully, fairly and transparently;
4. use accurate personal data;
5. use it for a specific purpose;
6. use no more than you need; and
7. only keep it for as long as you need it.

To help you to understand the law and good practice as clearly as possible, we explain in the code what you must, should or could do to comply.

- When we use the word **must** in the code, this refers to legal requirements.
- When we use the word **should** in the code, this does not refer to a legal requirement, but what we consider is important to help you to comply effectively with the law. You **should** do this unless there is a good reason not to. If you choose to take a different approach, you need to be able to demonstrate that your approach complies with the law.
- When we use the word **could** in the code, this refers to an option or options that you could consider to help you comply effectively. There are likely to be various other ways you could comply.

There are also Reference notes to support the code. Although not part of the code itself, these notes contain case law examples and refer to legal provisions and further reading.

How does this code take into account the special public interest in freedom of expression and information?

There is a strong public interest in a free press because it is vital to democracy. A free press can increase knowledge; inform debate; entertain and help citizens to participate in society. All forms of journalism can perform this crucial role, including local stories, entertainment news, and major investigations.

A free press is also a public watchdog that holds the powerful to account. It acts as an important check on political and other forms of power, particularly abuses of power.

Given the special role of freedom of expression and a free press, there is a broad exemption for those using personal data for journalism in data protection law. However, you **must** also consider this alongside other fundamental rights.

A degree of privacy, and limits on intrusion by the state and others with power, is needed to protect citizens' private and family life, their home and correspondence. This is fundamental to their physical, psychological and social well-being.

The protection of personal data is an important part of the broader right to privacy. It enables people to understand and exercise proportionate control over what happens to their personal data.

This code explains how to apply the key principles of data protection law flexibly and proportionately when considering these fundamental rights in a journalism context. This includes practical guidance about specific provisions to protect freedom of expression and information.

This code also takes into account consultation responses from industry and representative groups about the realities of news environments, which are often fast-paced, pressured and competitive.

How does this code relate to other codes and laws affecting the media?

This code does not concern media conduct or journalistic values in general. It is about data protection law and good practice. Media standards are covered by other industry codes including:

- Independent Press Standards Organisation (IPSO) Editors' Code of Practice;
- IMPRESS Standards Code;
- BBC Editorial Guidelines; and
- Ofcom Broadcasting Code.

However, this code is generally well-aligned with industry codes and is designed to complement industry guidance. Where relevant to data protection, we will take industry codes of practice into account and work with industry bodies.

Complying with industry codes will also help you comply with data protection law, as well as other privacy laws.

How will the ICO, a court or tribunal take this code into account?

This is a statutory code of practice under the DPA 2018. If someone complains about how you have used their personal data, the ICO, courts and tribunals must take this code into account once it is in force.

If you do not do what this code says you should do, you will need to be able to persuade the ICO or the courts that you have nevertheless complied with the law. Courts and tribunals will generally follow the guidance in codes and give weight to it unless there is a good reason not to.

How will the ICO review this code?

The ICO must review how personal data is used for journalism. This is not limited to the code, but the code will help us to consider compliance. We may also use the findings of the statutory reviews to help us update the code.

Complaints, enforcement and investigations

At a glance

- You **must** tell people about their right to complain when you provide privacy information.
- You **must** also tell people how to contact your Data protection officer (DPO), if you have one.
- Try to resolve complaints with the person concerned because this is likely to save you time and resources.
- If someone complains to the ICO, we can tell them whether it is likely you have complied with data protection law.
- There are several bodies who provide a complaints process about the media. We have published separate guidance to help people consider the most appropriate way to resolve their concern.
- People also have the right to enforce their data protection rights in court or claim compensation for damages, or both.
- Courts must stay (or in Scotland, sist) legal proceedings in some cases so data protection is not used to block publication.
- Any regulatory action we take is proportionate to the risks of harm involved. We also carefully consider the potential impact on freedom of expression before taking any action.
- To protect journalism, there are significant restrictions on our powers and procedural safeguards. There are also defences to criminal offences concerning journalism and the public interest.

In more detail

How should we deal with complaints about how we use personal data?

You **must** give people clear information about their rights and help them to use them. This includes details of their right to complain to the ICO and the courts (See Use personal data transparently).

If you have a DPO (see Take steps to protect personal data), you **must** make it clear how to contact them.

You **could** consider an online complaints form or publish a complaints policy to make it easier for people to contact you. If someone complains, you **should** consider it carefully. If you are able to resolve it directly, this may save you time and resources.

What happens if someone complains to the ICO or a court?

Before complaining to the ICO, we expect people to raise their concerns with you first. If we receive a complaint, we will consider whether it is likely you have complied with data protection law and we may ask you to take steps to put things right.

Our role is about data protection rather than general press standards. However, where there is overlap, we will work constructively with other regulators and industry bodies to resolve issues effectively and efficiently in line with our Regulatory action policy.

We also publish guidance for the public to help them complain about the media and consider the most appropriate organisation to make their complaint to.

People can enforce their data protection rights in court or claim compensation for damages, or both. When the case concerns journalism, the person pursuing court action can ask the ICO to assist, if the case is of substantial public importance.

Courts must stay (or in Scotland, sist) some legal proceedings if certain criteria are met, which protects publication.

What is the ICO's approach to enforcement and investigations and how is journalism protected?

We have powers to take formal enforcement action for breaches of data protection law. However, there are specific and strong protections for journalism and various restrictions and safeguards built into the law.

Any action we take will be targeted and proportionate in line with our Regulatory action policy. We reserve our strongest measures for incidents of serious harm. We also carefully consider the potential impact on freedom of expression before deciding to take any action in cases involving journalism.

We may also prosecute criminal offences. We only do this when we consider it is in the public interest in line with our Prosecution policy statement. There are specific defences available relating to the public interest and journalism.

The Reference notes contains more details about the key legal provisions.

1. Apply the journalism exemption

At a glance

- There is an exemption in data protection law to protect freedom of expression and information in journalism, academic activities, art and literature.
- When the criteria for using the exemption is met, you do not have to comply with many of the usual requirements of data protection law.
- You **must** always comply with the key data protection principles of accountability and security.
- The exemption applies if you:
  - use personal data for journalism;
  - act with the intention or hope of publishing journalistic material;
  - reasonably believe publication is in the public interest; and
  - reasonably believe that complying with a specific part of data protection law is incompatible with journalism.
- You **should** interpret journalism broadly.
- The exemption can cover all the personal data you use for journalism as long as you have the intention or hope of publishing it.
- A "reasonable belief" is one you are able to justify in a reasonable way.
- Deciding what is "in the public interest" involves considering the circumstances, balancing arguments for and against, and judging how the public interest is best served overall.
- The exemption applies if you reasonably believe that a specific part of data protection law must or should be set aside because complying with it disproportionately restricts your journalistic activity.

In more detail

What does the journalism exemption do?

1.1 There is an exemption in data protection law to protect freedom of expression and information in journalism, academic activities, art and

literature. For ease, we refer to this throughout the code as the journalism exemption.

1.2 When the criteria for using the exemption is met, you do not have to comply with many of the usual requirements of data protection law. For example, the exemption can remove the usual requirements to:

- have a lawful reason or basis for using data (see Use personal data lawfully);
- provide privacy information (see Use personal data transparently); and
- comply with individual rights that people have about their personal data (see Help people to use their rights).

1.3 For a full list of the parts of the UK GDPR that the exemption applies to, see key legal provisions in the Reference notes.

1.4 Although the journalism exemption is broad, you **must** always comply with some fundamental parts of data protection law, as follows:

- the principle of accountability, including the requirement to carry out a data protection impact assessment (DPIA) for certain types of processing (see Take steps to protect personal data);
- security (see Keep personal data secure);
- the right to opt-out of direct marketing;
- people's rights about automated processing;
- people's right to compensation for material or non-material damage; and
- registering with the ICO.

When can we use the journalism exemption?

1.5 The journalism exemption applies if you:

- use personal data for journalism;
- act "with a view to publication";
- reasonably believe that publishing is in the public interest; and
- reasonably believe that complying with a specific part of data protection law is incompatible with journalism.

1.6 In the following sections, we explain what each of these requirements means in practice.

1.7 In many cases, we anticipate that you will comply with data protection law when using personal data for journalism. However, there are some circumstances where, although you reasonably believe publication is in the public interest, data protection law may prevent or disproportionately restrict journalism. The exemption protects journalism in such circumstances.

When are we using personal data for journalism?

1.8 To rely on the journalism exemption, you **must** first decide whether you are using personal data for journalism. In many cases this will be obvious.

1.9 You **should** interpret journalism broadly to include:

- everything published in a newspaper or magazine, or broadcast on radio or television excluding paid-for advertising;
- content published by non-professional journalists, including members of the public (eg citizen journalism such as bloggers, eye witnesses or social networkers); and
- material that is journalistic but is also being used for another purpose, such as campaigning.

1.10 If you are not sure whether you are using personal data for journalism, you **should** consider the specific circumstances. Factors you **could** consider include:

- the purpose of the publication, including any reasons for publishing the information (eg informing the public);
- how closely the activity aligns with the media's traditional functions (eg holding the powerful to account);
- whether you have made some attempt to align with typical journalistic standards or values (eg checking accuracy);
- the content of the information, including any public interest in publication; and
- the extent to which you have, or will, promote the information to the public.

1.11 The above factors are not exhaustive and whether they are relevant, and the extent to which they are relevant, varies from case to case.

1.12 For third party content or online "user-generated content", you **could** consider whether you have applied any editorial judgement to the third party content (eg to decide whether to include a reader's response). The more editorial control exerted, the more likely it is that you are using personal data for the purposes of journalism.

When are we acting "with a view to publication"?

1.13 To rely on the exemption, you **must** also intend or hope to publish journalistic material. You publish material when you make it available to the public, even if it is not accessible to all members of the public (eg there is a subscription or pay wall).

1.14 Where you intend or hope to publish journalistic material, the journalism exemption can apply to all the personal data you collect, use or create as part of your journalistic activity.

1.15 It does not matter whether you actually publish the story you had in mind using the personal data. You can retain that personal data to use in a different story in the future, or update a story that you have already published (see Keep personal data only for as long as you need it).

What does "reasonable belief" mean?

1.16 To rely on the exemption, you **must** reasonably believe that:

- publication is in the public interest; and
- complying with the specific part of data protection law is incompatible with journalism.

1.17 You do not have to prove that publication is in the public interest or that complying with a specific part of data protection law is incompatible with journalism. Nor do you need to arrive at the same conclusion as the ICO or a judge. Different and opposing views may both be reasonable but you **must** be able to demonstrate the reasonableness of your decision.

1.18 In considering whether your belief is reasonable, it is not the role of the ICO or a judge to disregard your decision lightly or substitute their own belief in place of yours. They will only consider the reasonableness of your belief on an objective basis.

1.19 It is also not the role of the ICO or a judge to disregard the important editorial discretion that you have to decide how to edit, present and convey the information.

1.20 You **should** make an objectively reasonable decision. This is one that you are able to justify to another person in a reasonable way. You can make the decision yourself, where proportionate, or delegate as you see fit.

1.21 To make a reasonable decision, you **should** consider:

- whether you have enough relevant and reliable information to make a reasonable decision; and
- what weight to give to the information you take into account to help you make a proportionate decision.

1.22 It is the belief of the controller that is relevant rather than an individual journalist. However, you can decide to delegate responsibility for decisions to individual journalists depending on the level of risk.

Demonstrate your reasonable belief

1.23 You **must** be able to demonstrate that your belief was reasonable. There are different ways to do this, so you **should** decide what is appropriate depending on the circumstances. For example, you **could**:

- have a clear policy or process explaining who can make the decision and how;
- be ready to demonstrate that you followed your policy or process, as well as any relevant industry codes or guidelines; and
- keep a record of your decision. The level of risk involved will help you decide how detailed your records should be (see Take steps to protect personal data). You **could** do this at a later stage, if more appropriate.

What does "in the public interest" mean?

1.24 To rely on the exemption, you **must** reasonably believe that publication is "in the public interest".

1.25 To decide what is in the public interest, you **must** consider specific industry codes of practice or guidelines that are relevant to you. The DPA 2018 specifies the following codes:

- Independent Press Standards Organisation (IPSO) Editors' Code of Practice;
- BBC Editorial Guidelines; and
- Ofcom Broadcasting Code.

1.26 Although not listed in the DPA 2018, the IMPRESS standards code applies to its members.

1.27 To judge what is in the public interest, you **should**:

- consider the circumstances;
- balance relevant factors for and against publication; and
- judge how the public interest is best served.

1.28 You **should** consider whether the arguments in favour of publication are stronger than any harm to a person. Where there is a high risk, you **could** draw up a list showing the arguments on both sides to assess their relative weight.

General public interest arguments

1.29 There is a general public interest in freedom of expression and information and protecting people's right to privacy and data protection (see About this code).

1.30 The general public interest can take many forms. Examples you **could** consider include:

- upholding standards of integrity;
- ensuring justice and fair treatment for all;
- promoting transparency and accountability;
- encouraging public understanding and involvement in the democratic process; and
- securing the best use of public resources.

1.31 This does not mean that there cannot be a public interest in reporting on local events. What is ultimately "in the public interest" is determined by balancing factors in favour of publication against any harm to a person.

1.32 There may be a public interest in the general subject matter of the information. Examples you **could** consider include:

- protecting public health and safety;
- preventing people from being misled;
- exposing or detecting crime or anti-social behaviour; or
- exposing corruption, injustice, incompetence, negligence or unethical behaviour.

1.33 In general, there may be a stronger public interest for publishing information where a person:

- is a public figure (people who have a degree of media exposure due to their functions or commitments); or
- has a role in public life more broadly, where the public has an interest in having access to some information about them. Politicians, public officials, some business people and members of regulated professions are examples of people with this type of role.

Specific public interest arguments

1.34 As well as considering general public interest factors, you **should** also consider the specific circumstances and arguments both in favour and against publication.

1.35 Certain factors can add weight to the arguments on either side of the public interest balance. Factors you **could** consider include:

- how likely and severe any harm could be. If there would be a severe impact on people or other public interests, then this will carry significant weight in the public interest. This is relevant if, for example, there is any risk of physical or mental harm to an individual;
- the nature of the information and how likely it is to contribute to the public understanding. The information may enhance public debate, which may strengthen the public interest in publication; and
- whether information is already in the public domain. There may be a public interest in presenting a full picture or to remove any suspicion of manipulating the facts or spin. However, there may be a weaker public

interest in publication if similar information is already available and the information you wish to publish would not significantly add to it.

What does "incompatible with journalism" mean?

1.36 You **must** comply with data protection law if there is a straight-forward way to do so whilst still achieving your journalistic objective.

1.37 However, a part of data protection law may be "incompatible" with journalism if you reasonably believe that it must or should be set aside to enable your journalistic activity. As explained in section 1.20 of this code, a reasonable belief is one that you can objectively justify in a reasonable way.

1.38 In some cases, it will be obvious that you cannot carry out your journalistic activity and comply with data protection at the same time. For example, you cannot use personal data fairly and transparently if you decide to use covert methods as part of an undercover investigation (see Use personal data fairly).

1.39 If you are not sure whether part of data protection law is incompatible with your journalistic activity, you **should** consider what actions are proportionate in the circumstances. Generally, this means trying to achieve a fair balance between what you want to achieve and the interests of the individual.

1.40 Factors you **could** consider to help you to make a proportionate decision include:

- the extent to which your journalistic activity is restricted by complying with the specific part of data protection law;
- the extent to which your journalistic activity could harm the individual concerned;
- whether you could take steps to mitigate the impact on your journalistic activity whilst still complying with data protection law;
- whether you could reduce the impact of harm to the person whilst still achieving your journalistic objective; and
- overall, whether you believe that complying with the specific part of data protection law disproportionately affects your journalistic activity.

2. Take steps to protect personal data

At a glance

- You **must** take steps to protect personal data and be able to demonstrate that you comply.
- You **must** decide what steps to take to protect personal data. This varies depending on how you are using personal data for journalism and any risk of harm to people.
- You **must** review the steps you take to protect data and update them when you need to. Media organisations **could** take an organised approach to managing data protection by putting in place a system, sometimes known as a privacy management programme. This involves
  - strong leadership and oversight;
  - policies where proportionate;
  - training and awareness;
  - knowing what personal data you use; and
  - risk management.
- You **could** combine your approach to managing data protection with your existing management and governance systems.
- You **must** consider data protection when you do anything that involves personal data.
- You **must** identify and minimise risks when you use personal data. When there is likely to be a high risk, you **must** carry out a DPIA.
- **When the criteria applies, the journalism exemption can remove the usual requirement to consult us if a DPIA identifies a high risk that you cannot mitigate.**

In more detail

What does "take steps to protect personal data" mean?

2.1 This simply means you **must** proactively protect personal data and be able to demonstrate that you comply. This is sometimes known as the accountability principle.

2.2 There is no one-size-fits-all approach. It is for you to consider your circumstances and the level of risk to decide what steps are appropriate and

proportionate. Where proportionate to do so, you **must** put in place data protection policies.

2.3 When you have got measures in place, you **must** also review and update them when needed.

How can we make sure that we take the right steps to protect personal data?

Decide what is appropriate and proportionate

2.4 It is your responsibility to decide what measures are appropriate and proportionate in the circumstances. How much risk is involved is very important. You **must** consider:

- what personal data you are using, what you plan to do with it and why, as well as the wider context; and
- the risks of using the personal data – the higher the risks (eg of harm to people), the more important it is that you can clearly demonstrate how you comply.

2.5 Considering the wider context **could** involve taking into account:

- the size of your organisation;
- its overall structure;
- the resources available to you;
- your ways of working; and
- the special public interest in freedom of expression and information.

2.6 To consider the risks of using personal data for journalism, you **must** consider how much harm it could cause, and how likely it is to cause harm. This refers to harm to specific people as well as harm to wider society.

2.7 You **should** take into account significant risks, such as:

- discrimination, financial loss, damage to reputation or loss of confidentiality;
- stopping people from accessing their rights or controlling their personal data;
- using sensitive types of personal data known as special category data or criminal offence data (see Use personal data lawfully);
- physical harm;
- using personal data of vulnerable people, especially children; or
- using a large amount of personal data affecting a large number of people.

Demonstrate that you comply

2.8 To demonstrate what you do to comply with data protection law, you **should:**

- be able to give a clear and practical explanation of the steps you take to comply; and
- where appropriate and proportionate, provide evidence of what you do to comply and the measures you have put in place to ensure that this happens.

2.9 This code is generally well-aligned with industry codes so complying with them is likely to help you demonstrate that you comply with data protection.

2.10 You **could** adapt existing measures to take account of data protection requirements. For example, corporate risk, security and records management policies and existing editorial processes.

2.11 Where proportionate, you **must** put in place data protection policies, although this does not necessarily mean separate documents dealing solely with data protection. As above, you can incorporate data protection into your existing policies and processes.

2.12 You **must** also review what is happening in practice at appropriate intervals. You **should** consider not just what documentation you may have, but also how it is working for people.

2.13 Governance is often the name given to the framework of measures organisations use to comply with data protection and hold people to account. There are lots of different ways of doing this but you **could** consider adapting the ICO's Accountability framework and the main building blocks of an effective governance system or privacy management programme, as described below.

2.14 Smaller organisations or individuals are more likely to benefit from a smaller scale approach. See further reading in the Reference notes.

Leadership and oversight

2.15 Strong leadership and oversight of data protection are important to make sure you hold people to account appropriately.

2.16 You **should** set a positive tone and culture from the top by leading by example and making sure that your organisation complies with data protection.

2.17 You **must** have a DPO, if legally required. You **should** also be clear who is responsible for practical day-to-day data protection compliance at a senior level and below. For example, in job descriptions.

Policies

2.18 The UK GDPR specifically says that you **must** have policies, where proportionate. This is likely to be more important in environments where there is significant delegation from the top and where decisions are often made at pace, such as news environments.

2.19 What you may have policies for and their level of detail varies depending on what you think is proportionate. You **should** take the risk of harm into account amongst other relevant factors (see above).

2.20 For example, you **could** have a policy (either standalone or part of another policy) to help people understand how to use the journalism exemption. Your policy **could** set out:

- what the special purposes exemption does;
- when to apply it;
- how to apply it; and
- the roles and responsibilities people have when using it.

Training and awareness

2.21 You **should** make sure that staff receive the training on data protection that they need tailored to their role, including induction and refresher training.

2.22 You **should** also regularly raise awareness of data protection. For example, you **could**:

- create quick-reference guides;
- run internal campaigns; or
- draw attention to important information through your usual internal communication channels.

Know what personal data you use

2.23 Taking stock of what information you have, where it is and what you do with it, makes it much easier to put the right measures in place to protect personal data.

2.24 If you have 250 or more employees, you **must** record your use of personal data in line with legal requirements.

2.25 There is a limited exemption for smaller organisations with fewer than 250 employees. These organisations only need to record when they use personal data in ways that:

- are not just occasional;
- could result in a risk to people's rights and freedoms; or
- involve using special category or criminal offence data.

2.26 You **should** make sure that you adequately support data protection within your organisation by good records management.

Manage risk

2.27 You **must** integrate data protection into any system, service, product, policy or process you design that uses personal data. This is sometimes known as taking a data protection by design approach.

2.28 You **must** incorporate data protection into your normal practice, including:

- implementing the data protection principles effectively (see About this code);
- protecting individual rights (See Help people to use their rights); and
- using only the personal data that you need (see Use personal data for a specific purpose, Use no more data than you need and Keep personal data only for as long as you need it).

2.29 You **should** have appropriate measures in place to identify, record and manage personal data risks. For example, you **could** have a risk policy that is either a separate document or part of your wider corporate policy.

Data protection impact assessments

2.30 A DPIA is simply a type of risk assessment. The UK GDPR provides significant flexibility to decide what structure and form it takes so that it fits with your existing processes. As a minimum, a DPIA **must**:

- describe how you plan to use the personal data and why;
- assess whether it is necessary and proportionate to use the personal data;
- assess the risks to the rights and freedoms of the people whose personal data you wish to use; and
- set out how you intend to manage these risks.

2.31 You do not need to do a DPIA every time you use personal data for journalism, but you **must** do a DPIA whenever you use personal data in a way that is likely to result in a high risk to someone. You **could** also do a DPIA for any other major project involving personal data.

2.32 You do not need to carry out a DPIA for individual stories. You **could** do a more general DPIA that covers the ways you may use personal data in high risk ways (eg using personal data for investigative journalism).

2.33 Assessing risk involves considering how likely it is that using personal data will cause harm and how severe any harm could be (see Take steps to protect personal data). Much of the day-to-day work of journalists does not involve a high risk to people. If you think there may be a high risk, you **must** consult your DPO, if you have one.

3. Keep personal data secure

At a glance

- You **must** keep personal data secure. This involves protecting personal data against unauthorised or unlawful use and accidental loss, destruction or damage.
- Security measures are not limited to cyber-security. They also include organisational measures and physical security.
- You **must** be able to restore personal data if there is a security incident.
- You **must** review and keep security measures up-to-date.
- You **must** decide what security measures are appropriate and proportionate to protect personal data, taking into account the circumstances, the risk of harm, and available technology.
- Your security arrangements **should** take into account the security risks of using mobile devices and remote working.
- You **must** ask anyone acting on your behalf to demonstrate they can keep personal data secure. You **must** also have a written contract with them dealing with security.
- A DPIA can help you assess security risks when others act on your behalf or you share personal data with them.
- You **must** record all personal data breaches, and tell the ICO if the breach is likely to cause harm to someone.
- If there is a high risk, you **must** also tell the people affected.
- **When the criteria applies, the journalism exemption can remove the usual requirement to tell people affected by a data breach when there is likely to be a high risk.**

In more detail

What does keeping personal data secure mean?

3.1 You **must** keep personal data secure. This involves protecting it against unauthorised or unlawful use and accidental loss, destruction or damage.

3.2 To do this, you **must** have appropriate and proportionate security measures. This involves cyber-security, as well as physical and organisational security measures.

3.3 You **must** be able to restore personal data if there is a security incident as soon as possible (eg a backup system).

3.4 You **must** also review and update your security measures. For example, scanning for network vulnerabilities to prevent risks developing that compromise your security.

How do we keep personal data secure?

Decide what security is appropriate and proportionate

3.5 In a similar way to the accountability principle, you **must** consider all the circumstances and the risks of harm to keep personal data secure (see Take steps to protect personal data). You **must** also take into account what technology is available and the costs of security measures.

3.6 You **should** consider factors such as:

- your organisation's premises and computer systems;
- who has access to personal data and how; and
- any personal data a third party is using on your behalf.

Harm

3.7 Amongst other factors, you **must** consider how likely it is that using the data could harm someone, and how severe any harm could be.

3.8 When choosing security measures, you **should** consider significant risks. You **must** also carry out a DPIA, if there is likely to be a high risk. This will help you decide on appropriate security measures to manage the risks.

3.9 For example, there is a high risk involved in personal data that could identify a journalist's confidential sources. In some cases, a security breach could pose a risk to someone's physical health or safety. Where that is the case, you **should** have strong security measures to protect the personal data, including strict measures controlling access.

Working practices

3.10 Journalism often involves working flexibly in different environments, including a strong reliance on remote working and portable devices. You **should** therefore consider how you keep your IT equipment secure, especially portable devices, such as laptops, tablets, and smart phones.

3.11 There are a wide range of low-cost and easy to implement cyber-security solutions. You **should** consider common techniques such as encryption and password protection. This is important for all the devices you use, including mobile ones.

3.12 Where you have a business need to store personal data on removeable media (eg a memory stick), you **must** minimise it (see Use no more data than you need).

3.13 You **should** consider the increased security risks if you allow employees to use their own devices for work purposes.

3.14 You **should** train your employees to follow fundamental security advice if travelling with personal data, including:

- check Foreign Office travel advice, if going overseas;
- only take what you need;
- keep devices and papers with you and store them securely; and
- lock or power off your device when not in use.

3.15 You **should** also raise awareness of common security issues when travelling, such as discussing confidential information, allowing people to overlook a screen and writing down or telling someone a password.

Third parties using data on your behalf

3.16 You **must** make sure that any third parties acting on your behalf and using personal data comply with the UK GDPR (see Be clear about roles and responsibilities).

3.17 In particular, you **must** only use third parties to act on your behalf that can give you sufficient guarantees about their security measures to protect personal data.

3.18 You **must** have a written contract with the third party, making it clear that they must provide the same level of security for personal data as you do. The contract **should** allow you access to all the information you need to demonstrate that the personal data is secure.

Sharing personal data

3.19 You may share personal data with a third party who is not acting on your behalf. For example, you may ask a freelance journalist to write a story or take a photograph, where they have the freedom to act beyond your instructions. In this scenario, the third party is also legally responsible for keeping the personal data secure in the same way as you are.

3.20 Even if you are not legally required to do a DPIA, you **could** do one when sharing personal data to help you to identify security risks and how to mitigate them. This may be particularly helpful if the data sharing is routine or planned, when you may have more time available.

Personal data breaches

3.21 You **must** keep a record of personal data breaches and how you deal with them. A personal data breach means a breach of security leading to the

accidental or deliberate destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

3.22 If a personal data breach is likely to cause harm to someone, you **must** tell the ICO as soon as possible, and generally within 72 hours. If you do not think the breach is likely to cause harm, you **should** record the reason.

3.23 You **must** tell people affected by a breach when there is likely to be a high risk to them.

4. Use personal data lawfully

At a glance

- You **must** use personal data lawfully.
- You **must** have a specific lawful reason under the UK GDPR to use personal data.
- The lawful reasons most likely to be relevant to journalism are legitimate interests and consent.
- You have a legitimate interest in using personal data, if there is not a less intrusive way of achieving the same result, and your interests are not outweighed by harm to a person.
- Consent is often not the most appropriate lawful reason for a journalist to use, unless you are giving people genuine control over how you use their data. If you rely on consent, you **must** comply with the high standards of consent in the UK GDPR.
- Special category or criminal offence data needs more protection because it is sensitive. You can use this type of data, if you have a lawful reason **and** can satisfy the relevant conditions and safeguards under the DPA 2018.
- If the criteria is met, there is a condition to enable sources to disclose these sensitive types of data about unlawful acts and dishonesty for journalism.
- Criminal offence data includes allegations of criminal behaviour. You **should** consider all the circumstances to decide if a suspect has a reasonable expectation of privacy. If a suspect is under investigation by the state, there is usually a reasonable expectation of privacy.
- You **should** make sure you can justify identifying a suspect, taking into account the public interest in publication and the harmful consequences for the person.
- **When the criteria applies, the journalism exemption can remove the usual requirements to:**
  - **use personal data lawfully in line with the data protection principle;**
  - **satisfy a lawful basis for using the data;**
  - **comply with conditions for consent and children's consent; and**
  - **comply with the rules about special category data and criminal offence data.**

In more detail

What does use personal data lawfully mean?

4.1 You **must** have a specific lawful reason for using personal data. This is known as a lawful basis, or bases, if more than one applies.

4.2 You can use sensitive types of data known as special category data and criminal offence data, if you can satisfy the relevant conditions and safeguards.

4.3. If you are using special category data, you **must** have a lawful reason and satisfy a separate condition. For some of these, you **must** also meet additional conditions and safeguards that are set out in Schedule 1 of the DPA 2018.

4.4 If you are using criminal offence data, you **must** have a lawful reason and satisfy a relevant condition under Schedule 1 of the DPA 2018.

4.5 You **must** check that you are acting in line with other laws as well, including statutory and common law obligations, whether criminal or civil. For example, using personal data may be unlawful if it is a breach of confidence, the Human Rights Act 1998, or in contempt of court.

How do we use personal data lawfully?

4.6 You **should** use the most relevant lawful reason and consider if more than one applies. Changing your mind about which lawful reason applies is likely to breach the data protection principle to use personal data fairly and transparently.

4.7 The lawful reasons most likely to be relevant to journalism are legitimate interests and consent. Although, legitimate interests is often more appropriate than consent in most cases.

Legitimate interests

4.8 You can rely on this lawful reason when it is necessary to use personal data to pursue legitimate interests **and** where those interests are not outweighed by any harm caused to a person.

4.9 This lawful reason is likely to be most appropriate when you use people's personal data in ways they would reasonably expect with minimal privacy impacts. For example, in day-to-day reporting on local events. However,

even if there is a more significant risk of harm, it can still apply if you can justify the harm.

4.10 If you want to use this lawful reason, you **should** identify what your legitimate interests are. Legitimate interests can be your own or third party interests. For example, there is a legitimate interest in journalism because of the special public interest in freedom of expression and information (see About this code).

4.11 You **must** only use the personal data if it is necessary. This means that you **should** consider whether there is another reasonable and less intrusive way to achieve the same result. If there is, this lawful reason does not apply.

4.12 You **must** consider whether your legitimate interests are outweighed by harm to a person. You **should** consider their reasonable expectations and any unwarranted harm (see Use personal data fairly). You **could** complete a Legitimate interest assessment to help you balance different interests.

4.13 You **should** take extra care when dealing with children's personal data or other vulnerable groups. You **must** consider a child's best interests in accordance with the United Nations Convention on the Rights of the Child.

Consent

4.14 The consent lawful reason may sometimes be used for journalism. For example, you can use special category data with explicit consent (see below).

4.15 However, consent is often not the most appropriate lawful reason to use for journalism, unless you are giving someone genuine choice and control over how you use their personal data.

4.16 If you want to use a child's personal data, you **should** consider the child's competence and ability to understand consent. If you have doubts, the legitimate interests lawful reason may be more appropriate to show that you have properly protected the child's rights.

4.17 When offering an online service directly to children, only children aged 13 or over are able to consent.

4.18 If you are relying on consent as a lawful reason for using personal data, you **must** comply with the high and specific standards for consent in the UK GDPR. You **could** keep a record of who consented, when, how and what you told them to help demonstrate that you have complied (See Take steps to protect personal data).

What is special category data?

4.19 Data protection law gives extra protection to sensitive types of personal data. Some of this type of data is known as special category data.

4.20 Special category data is personal data revealing or concerning information about:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- health;
- sex life; or
- sexual orientation.

4.21 You can use special category data for journalism if you have a lawful reason for doing so **and** you meet one of the conditions in the UK GDPR. For some of these, you **must** also meet further conditions and safeguards set out in Schedule 1 of the DPA 2018.

How do we use special category data lawfully?

4.22 First, you **should** decide whether you are using special category data. The UK GDPR is clear that the information does not need to specify these details. Information that reveals or concerns special category data is also covered.

4.23 There may be times when you are not sure whether the information is special category data. For example, you may be able to infer an individual's religion or ethnicity from names, photographs or film. Where there is doubt, you **should** consider:

- whether it is possible to infer or guess special category data from the information you want to use;
- how certain that inference is; and
- whether you are deliberately inferring the data.

4.24 If you use the personal data specifically because it reveals one of the details above, you are using special category data. However, if you can only infer or guess these details, you do not need to meet extra conditions to use the data. Although you **must** still consider whether it is fair to use the information in context (see Use personal data fairly).

4.25 Before you use special category data, you **should** consider why you want to use it. This will help you choose a lawful reason and condition, and where relevant, a further condition and safeguard.

4.26 There are 10 conditions under the UK GDPR that provide extra protection for special category data and can give you a valid reason for using it. Below, we refer to those most likely to be relevant to journalism.

Explicit consent is given to use it

4.27 As well as meeting the high standard of consent that is required by the UK GDPR generally, explicit consent is also expressly confirmed in words.

The data is manifestly made public by the person it is about

4.28 This condition applies if personal data is obviously made public by the person concerned. Personal data is made public if it is realistically accessible to a member of the general public, including if that is only to part of the general public because there is, for example, a subscription or paywall to access news content. This condition does not apply if an individual has indicated an intention to make it public in the future or is in the process of doing so.

4.29 You **should** be cautious when applying this condition to information obtained from social media posts or other user-generated content. You **must** always consider whether it is fair to use the data, bearing in mind that people may make their personal data public without realising it.

4.30 In the context of criminal trials, an offender may obviously make information about their offending public in line with the principle of open justice. However, you **must** consider whether using the personal data remains fair at a later date. An offender may reasonably expect privacy as a result of the passage of time, even if information is initially made public.

4.31 You **should** also consider whether using the personal data would cause unwarranted harm. There is a strong public interest in the rehabilitation of offenders recognised in the Rehabilitation of Offenders Act 1974 (ROA 1974). Although this is generally a strong factor in favour of not publishing or broadcasting data once a conviction is spent, whether or not it is fair depends on all the circumstances.

There is a substantial public interest with a reason in law

4.32 You can use special category data if there is a substantial public interest and you have a valid legal reason to do so. This means that one of the substantial public interest conditions **must** apply that is set out in paragraphs 6 to 28 of Part 2 of Schedule 1 of the DPA 2018.

4.33 There are 23 substantial public interest conditions. We refer below to the two conditions most likely to be relevant to journalism.

It is necessary for the administration of justice

4.34 This condition is met if using personal data is necessary for the administration of justice.

4.35 The open justice principle is a long-standing feature of our legal system that recognises the strong benefits to society of open justice. For example, promoting public confidence in, and respect for, the administration of justice.

4.36 If you use this condition, you **must** have an Appropriate policy document. You **must** keep this for six months after you stop using the data. You **could** publish it to help people understand how you protect personal data.

It is disclosed for journalism about unlawful acts and dishonesty

4.37 This condition is most likely to be used to allow a person or an organisation, such as a whistle-blower, to send data to you for the purposes of journalism.

4.38 It applies if special category data is **disclosed** for journalism by the person with legal responsibility for complying with data protection law known as the controller **and** it relates to:

- a person acting unlawfully;
- dishonesty, malpractice or other seriously improper conduct of a person;
- the unfitness or incompetence of a person; or
- mismanagement or service failure by a body or association.

4.39 The controller of the personal data can disclose personal data to you for journalism if there is a substantial public interest, it is necessary to disclose the data, and they:

- are disclosing it with a view to publication; and
- reasonably believe that disclosure of the personal data would be in the public interest.

4.40 If a third party controller uses this condition to disclose personal data to you, you need to apply the journalism exemption, if you want to use the data for journalism yourself (see Apply the journalism exemption).

What is criminal offence data?

4.41 Data protection law gives extra protection to personal data about criminal convictions and offences or related security measures. This is sometimes known as criminal offence data.

4.42 Criminal offence data covers a wide range of information about:

- criminal activity;
- allegations;
- investigations; and
- proceedings.

4.43 It also covers related security measures, including:

- personal data about penalties;
- conditions or restrictions placed on someone as part of the criminal justice process; or
- civil measures which may lead to a criminal penalty, if not adhered to.

4.44 You can use criminal offence data for journalism if you have a lawful reason for doing so and you meet one of the conditions in Schedule 1 DPA.

How do we use criminal offence data lawfully?

4.45 Before you use any criminal offence data, you **should** consider why you want to use it. This will help you choose a relevant lawful reason and condition.

4.46 There are 28 conditions that allow you to use criminal offence data that are set out in paragraphs 1 to 37 of Schedule 1 of the DPA 2018. Those most likely to be relevant to journalism are the same as those set out above about special category data. The only difference is that consent does not need to be explicit.

Allegations of criminal activity

4.47 Before you use personal data about allegations of criminal activity, you **must** consider a person's reasonable expectations of privacy and the serious risk of harm, in particular, reputational harm. You **must** do this if you are considering whether:

- the legitimate interests lawful reason applies;
- using the data would be fair; and
- the journalism exemption applies.

4.48 In some cases, there may be a risk of prejudice to the course of justice. You **must** only use criminal offence data if it would not breach any other law. For example, you may be in contempt of court if you publicly comment on a court case on social media or in a story.

4.49 A suspect under state investigation usually has a reasonable expectation of privacy up to the point of charge, including about the fact that there is an investigation. Although it depends on the specific facts of each case, the facts will often point to a conclusion that there is a reasonable expectation of privacy.

4.50 Whether or not someone is under a state investigation, you **should** consider whether they have a reasonable expectation of privacy in all the circumstances (see Use personal data fairly). There may be reasons why an expectation of privacy is not reasonable. For example:

- the activity may take place in a public place where it is not reasonable to expect privacy (eg rioting);

- an expectation, that was initially reasonable, may no longer be so (eg if the police decide to disclose information for operational reasons).

4.51 When considering where an activity, such as an arrest, took place and any resulting impact on privacy expectations, you **should** take into account that media reporting can attract substantially more attention than would otherwise be the case.

4.52 You **should** make sure you can justify any decision to publish information identifying a suspect, taking into account the public interest in publication and the harmful consequences for the suspect (see Apply the journalism exemption).

4.53 You **should** act proportionately and consider whether you can sufficiently serve the public interest without identifying the suspect. For example, you may be able to highlight weaknesses in an investigation by a public authority without identifying a suspect.

4.54 If there is a duty of confidence associated with the personal data, you **should** take into account that there is a strong public interest in observing duties of confidence. For example, documents about a public authority's investigation of criminal activity.

4.55 It **could** be relevant to consider the impact of a person's public profile because they may be more vulnerable to false allegations. An allegation that causes reputational harm may also be more damaging to such people because of their public status and the specific circumstances.

5. Use personal data fairly

At a glance

- You **must** use personal data fairly.
- You **should** consider what someone reasonably expects in the circumstances and whether using the data is likely to cause any unwarranted harm.
- You **should** consider the specific circumstances to decide what someone reasonably expects. Various factors may be relevant including:
  - the extent to which the information is in the public domain;
  - a person's public profile; and
  - the risk of harm.
- There are certain types of sensitive data that will normally, but not always, be private, such as data about a person's physical or mental health and sex life.
- When someone is charged with a crime, the open justice principle means there is generally an expectation of transparency, although this data may become private with the passage of time.
- You **should** make sure you can justify your decision to use any personal data in view of the risk of harm and publish data that is proportionate to the public interest.
- Photographs or filming may be particularly intrusive. You **must** consider whether it is fair to use the data, even if the person is in a public place.
- Using covert surveillance, subterfuge or similar intrusive methods may be justified in the context of journalism, but you are likely to need to use the journalism exemption.
- **If the criteria applies, the journalism exemption can remove the usual requirement to use personal data fairly.**

In more detail

What does using personal data fairly mean?

5.1 You **must** use personal data fairly. This involves using it lawfully and transparently, which are part of the same data protection principle (see also Use personal data lawfully and Use personal data transparently).

How do we use personal data fairly?

5.2 You **should** use personal data in ways that:

- people reasonably expect; and
- do not cause unwarranted harm to them.

5.3 Not all harm is unwarranted. You can use personal data even if it may cause harm but you **should** be able to justify it. The greater the harm, the stronger your justification should be.

Reasonable expectations

5.4 You **should** consider whether using personal data is within someone's reasonable expectations, taking into account all the circumstances.

5.5 When considering a person's reasonable expectations, it is often important to decide whether a reasonable person would consider the information to be private.

5.6 When in doubt about whether someone has a reasonable expectation of privacy, you **could** consider the following factors:

- the person concerned (eg Are they an adult or a child? Are they a public figure or do they perform a public role?);
- the nature of the activity and where it happens;
- how and why you plan to use the data;
- your lawful reason for processing the data;
- the impact on the person; and
- how and why you obtained the personal data.

5.7 If a person is acting in the context of professional or business activities, there may be no reasonable expectation of privacy or it may be reduced significantly. However, they may still reasonably expect privacy, so you **should** consider all the circumstances.

5.8 Information that was private may become so well-known that it is no longer private. If the information, or similar information, about the person is already in the public domain, the impact on any reasonable expectation of privacy varies depending on the facts and circumstances.

5.9 A public figure may attract or seek publicity about some aspects of their life without necessarily losing the right to privacy in other matters. You **should** consider all the circumstances. Factors you **could** take into account include:

- the extent to which someone has made their personal data public;
- what personal data they have made public; and
- how you are planning to use their personal data.

Sensitive types of personal data

5.10 While you **should** always consider all the circumstances, there are certain types of information which are usually, but not always, considered private. For example:

- special category data is a sensitive type of data that is given extra protection under the UK GDPR (see Use personal data lawfully);
- personal data about someone's home life, correspondence or personal finances; and
- personal data about someone's involvement in crime as a victim or a witness.

5.11 Criminal offence data is also given extra protection in the UK GDPR. However, the principle of open justice means that the media can generally report on criminal trials (see Use personal data lawfully).

5.12 You **should** make sure you can justify any harm caused to someone. In particular, there is a greater risk of harm when using special category data because it is more likely to harm a person's fundamental rights. For example, it could cause discrimination.

5.13 Any time you use personal data, whether or not it falls within the sensitive types protected by the UK GDPR, you **must** consider the risk of harm to people (see Take steps to protect personal data).

Children and other vulnerable people

5.14 You **must** take extra care when dealing with children's personal data (anyone under 18). The child's best interests **must** be your main consideration in accordance with the United Nations Convention on the Rights of the Child.

5.15 You should also take into account other groups who may be vulnerable, such as some elderly people or those with certain disabilities.

5.16 All these groups may be less able to understand how you will use their data and the risks involved. In these circumstances, publication is less likely to be fair.

5.17 A child does not have a lower expectation of privacy simply because their parents have a public profile.

Photographs or filming, especially in public

5.18 You **should** keep in mind that photographs or film may be particularly intrusive. The intrusive impact may be greater if someone is continually

photographed or recorded, or if it was not clear to them what you were doing.

5.19 People should reasonably expect that they may sometimes be photographed or caught on film in public in an incidental way. However, if a person's image is captured in public and they are the subject of the photograph or film, you **must** consider whether using their personal data is fair in the circumstances, even if the activity is happening in a public place.

5.20 You **should** act proportionately, taking into account the public interest in using the personal data and the harm it could cause. You **should** consider whether the public interest can be sufficiently served without disclosing the specific personal data shown in the photograph or film.

Covert surveillance, subterfuge and similar intrusive methods

5.21 These types of techniques include the use of private detectives, covert recording, disguise, and long-lens photography. Such methods are more likely to be used for investigative journalism.

5.22 You **should** consider whether it is proportionate to use these kinds of methods to serve the public interest, or whether there is a less intrusive way of doing it.

5.23 If you are using covert and intrusive methods, you are likely to need to use the journalism exemption (see below). This is because such techniques are unlikely to be in line with the data protection principles to use personal data fairly and transparently, although they may still be justified in the context of journalism.

5.24 You **should** carefully consider the strength of the public interest in publication and take into account harm to the person concerned. Given the risk of harm, it is more likely to be appropriate to record your decision and the factors you considered. There is generally a greater risk of harm if you are using special category data, such as details about an individual's sex life or criminal offence data.

6. Use personal data transparently

At a glance

- You **must** use personal data transparently.
- You **must** tell people about your use of their personal data. This information is known as privacy information.
- When you collect personal data from the person it is about, you **must** provide them with privacy information at the time you collect it.
- When you collect personal data from a source other than the person it is about, you **must** provide that person with privacy information within a reasonable period and no later than one month.
- You **must** make people aware of privacy information and it must be easy to understand and access, especially if you use personal data about children or vulnerable people.
- When you collect personal data from a source other than the person it is about, you do not need to provide information if an exception applies, including that it would be impossible, involve disproportionate effort or cause serious prejudice to your journalistic aims.
- You **should** consider whether you need to do a DPIA if you collect personal data from a source other than the person it is about without providing them with privacy information.
- **When the criteria applies, the journalism exemption can remove the usual requirements to:**
  - **use personal data transparently; and**
  - **provide privacy information to the person the personal data is about when you collect it.**

In more detail

What does "use personal data transparently" mean?

6.1 You **must** use personal data transparently to help people understand data protection and exercise control over their personal data.

6.2 In particular, you **must** generally provide information to people about your use of their personal data. This is called privacy information.

6.3 When you collect personal data from the person it is about, you **must** provide privacy information at the time you collect it unless they already have it.

6.4 When you obtain personal data from a source other than the person it is about, even if it is a publicly accessible source, you **must** provide that person with privacy information within a reasonable period. It should not be later than one month. If you are contacting the person the data is about, or plan to disclose or publish the data, you **must** provide privacy information when you make contact or disclose the data at the latest.

6.5 When you obtain personal data from a source other than the person it is about, you do **not** need to provide privacy information if:

- the person already has the information;
- providing the information would be impossible;
- providing the information would involve a disproportionate effort;
- providing the information would make it impossible or seriously impair your ability to achieve your objectives;
- you are required by law to obtain or disclose the personal data; or
- you are subject to an obligation of professional secrecy regulated by law that covers the personal data.

How do we process personal data transparently?

6.6 You **must** provide privacy information at the time you collect personal data or within a reasonable period, as explained above. This means acting fairly in the circumstances and giving people a meaningful opportunity to consider privacy information, where possible.

6.7 The privacy information you provide **must** be concise and easy to understand, especially when you are using children's data or data about vulnerable people. There are a variety of different techniques. For example, you **could** consider using graphics and videos.

6.8 You **must** actively provide privacy information. If you have a website, you **should** include a privacy notice and you **should** also consider whether you need to provide privacy information in other ways to make sure it is easily accessible.

7. Use accurate personal data

At a glance

- You **must** use personal data that is accurate and, where necessary, keep it up-to-date.
- You **must** take reasonable steps to check that personal data is accurate.
- You **should**:
  - make sure that the source of the personal data and their status is clear, where possible;
  - consider any challenges to the accuracy of the data; and
  - consider whether you need to update it.
- As a general rule, the greater the risk of harm to people, the more thorough your accuracy checks need to be.
- If normal accuracy checks are not possible, you **should** make sure your staff know how to manage the risk of harm.
- You **should** consider how accurate the sources of personal data are.
- You **should** clearly distinguish between fact and opinion when reporting personal data.
- You **should** clarify the nature or context of personal data where necessary.
- You **must** help people to exercise their data protection rights if they challenge the accuracy of personal data.
- **When the criteria applies, the journalism exemption can remove the usual requirement to use accurate personal data.** However, accuracy is generally a fundamental journalistic value so you are unlikely to use it for this reason often.

In more detail

What does use accurate personal data mean?

7.1 You **must** use personal data that is accurate and, where necessary, keep it up-to-date. You **must** also take reasonable steps to make sure that personal data is accurate.

7.2 The DPA 2018 says that "inaccurate" means "incorrect or misleading as to any matter of fact".

How do we make sure that personal data is accurate?

Reasonable accuracy checks

7.3 Even in lower profile stories, you **must** take reasonable steps to check that personal data is accurate. Simple accuracy checklists **could** help you to do this when working at pace.

7.4 You **should**:

- make sure that the source of the personal data and their status is clear where possible;
- consider any challenges to the accuracy of information; and
- consider whether you need to update the data.

7.5 To help you decide what accuracy checks are reasonable, you **should** consider the circumstances, including the urgency of the particular story and the risk of harm. As a general rule, the greater the risk of harm to someone, the more thorough your accuracy checks should be.

7.6 There may be circumstances when you decide that it is in the urgent public interest to publish personal data without carrying out normal accuracy checks. This may be the case when broadcasting live, for example. You **must** be able to show that you put in place appropriate measures to manage the risks (see Take steps to protect personal data). You **could** consider the following factors:

- who has authority to make the decision;
- what checks might be possible;
- whether you could delay publication;
- the nature of the public interest at stake; and
- the risk of the information spreading quickly online.

7.7 If you go ahead with publication or broadcast in the above circumstances, you **should** be as clear as possible that you are reporting on unconfirmed facts and any potential inaccuracies.

Sources of information

7.8 You **should** consider how accurate the sources of personal data are. A clear process for checking facts and sources **could** help you to do this. For example, you **could** consider whether you are dealing with:

- a primary source (who you hear from directly);
- a generally reliable source such as a news agency; or
- a secondary source (typically a second-hand report by someone else).

7.9 Primary sources may be more reliable generally. For example, you may feel confident in the eye-witness account of a colleague working within your organisation or in an interview broadcast by another news outlet. However,

you **must** still carry out reasonable checks (eg if you have several different accounts from eye-witnesses).

7.10 Secondary sources may be less reliable than a primary source. This may be a tip-off, comments on social media or something reported to have happened by another news outlet. You **should** take particular care when using online material, especially social media or other user-generated content.

7.11 You **should** consider what steps it is reasonable to take to check and corroborate what a source has told you or put the data into its appropriate context (see below).

7.12 If possible, you **should** be clear about the source of the personal data you use to help the public judge their status and credibility. When you need to protect a source, you may still be able to provide some general information (eg about their status). You should not say anything inaccurate about a source's status.

7.13 Wherever appropriate and proportionate, you **should** keep records about your sources and other research that you use to report someone's personal data. This allows others to verify the accuracy of the information you use where necessary, such as if there is a later dispute.

Facts, opinions and context

7.14 You **should** clearly distinguish between fact and opinion when reporting personal data. Some programmes may involve a blend of factual and fictional elements about people, so you should make the extent of the facts clear.

7.15 You **could** consider how the words would strike the ordinary reasonable reader, taking into account their context and the subject matter when determining whether the personal data is a fact or an opinion.

7.16 While deciding what editorial position to take when reporting the news, it is important to make sure you continue to present personal data accurately. You may need to clarify the nature or context of some content specifically to avoid compromising the accuracy of the personal data. For example, you **should** check that headlines are supported by the text.

7.17 If personal data is deliberately inaccurate and this is obvious from the context, such as satirical or parody articles, this is unlikely to breach the accuracy principle.

Complaints and corrections

7.18 You **must** help people to exercise their individual rights under data protection law (see Individual rights). You **should** be clear with people about how they get in touch with you if they believe you have published or broadcast inaccurate personal data about them, and how you will consider the issue (see Complaints, enforcement and investigations).

7.19 Recording inaccuracies and monitoring any recurring themes **could** help you to review your processes and make improvements where needed.

Updating personal data

7.20 To decide whether you need to update data, you **should** consider what you are using it for. If the data needs to be current for you to use it, you **should** take proportionate steps to keep it up-to-date. For example, updating your contacts book if someone tells you they have new contact details.

8. Use personal data for a specific purpose

At a glance

- You **must** use personal data for a specific purpose that is legitimate, clear and in line with your original purpose.
- To comply with this principle, you **must** also use personal data fairly, lawfully and transparently and be accountable for how you use it.
- You can use data for another purpose, if it is in line with your original purpose.
- Keeping a news archive is part of the end-to-end process of journalism so there is no change in purpose.
- If you are using data for a purpose that is very different, unexpected or which would have an unjustified impact, this is not likely to be in line with this data protection principle. However, you **could** consider whether you could get consent to use the data.
- **When the criteria applies, the journalism exemption can remove the usual requirement to use personal data for a specific purpose.**

In more detail

What does using personal data for a specific purposes mean?

8.1 You **must** use personal data for a specific purpose that is legitimate, clear and in line with your original purpose, or which is "compatible".

8.2 This data protection principle is closely linked to other principles. To comply with it, you **must** also:

- be clear about why you are using the data (see Use personal data transparently);
- be able to demonstrate the steps you take to protect data, in particular by recording why you are using personal data (see Take steps to protect personal data); and
- use personal data fairly, lawfully and transparently, if you plan to use it for a new purpose (see Use personal data lawfully, Use personal data fairly, and Use personal data transparently).

How do we make sure that we use personal data for a specific purpose?

8.3 You **must** use personal data fairly, lawfully and transparently. If you do this, you are also likely to comply with the principle to use data for a specific purpose.

8.4 If you comply with your other obligations to be transparent and accountable, you are unlikely to need to do anything more to specify your purposes for using personal data. In particular:

- you **must** provide privacy information to people unless an exception applies; and
- if you have 250 or more employees, you **must** keep records about how you use personal data in line with legal requirements.

8.5 You **must** review how you use personal data and your privacy information to check that your purposes have not changed over time. Sometimes this can happen gradually, known as function creep.

Using personal data for another purpose

8.6 You can use personal data for a new purpose, if it is in line with your original purpose.

8.7 Keeping personal data for a news archive is still using personal data for journalism because this is part of the end-to-end process.

8.8 Factors you **should** take into account when considering if you may use personal data for a new purpose include:

- any link between the original purpose and the new purpose;
- how you collected the information and the reasonable expectations of the people concerned;
- the nature of the personal data and any harm to people;
- how you have kept the data safe and how you will continue to keep it safe.

8.9 If you are using data for a purpose that is very different, unexpected, or which would have an unjustified impact on people, this is not likely to be in line with this data protection principle. However, you **could** consider whether the person will consent to the new use (see Use personal lawfully).

9. Use no more personal data than you need

At a glance

- You **must** have enough personal data to do what you need to do and it **must** be relevant and not excessive.
- Before you collect any personal data, you **should** think about why you need it.
- You **should** think about any factors people bring to your attention when exercising their rights that may suggest you are not using the right amount of personal data.
- You **must** use accurate personal data for journalism, which also involves considering how much data you need.
- You **should** keep in mind what you are trying to achieve and aim to collect the data you need to do that efficiently.
- You **must** use personal data that is relevant to your story or your wider journalistic purpose. Using irrelevant personal data, particularly sensitive types of data, can cause significant harm to people (eg discrimination).
- You **must** use personal data in limited ways (ie not use excessive data).
- You **should** think about whether you need to collect personal data and whether you also need to use it in other ways.
- You **must** review any data you keep from time to time to make sure you do not keep it for longer than you need to.
- **When the criteria applies, the journalism exemption can remove the usual requirement to use no more personal data than you need.**

In more detail

What does use no more data than you need mean?

9.1 You **must** have enough personal data to do what you need to do, and it **must** be relevant and not excessive. This is known as the data minimisation principle.

9.2 You **must** use personal data that is:

- **adequate** (enough to do what you need to do);

- **relevant** (has a rational link to that purpose); and
- **limited** (you do not hold more than you need for that purpose).

How do we make sure that we use no more data than we need?

9.3 Before you collect any personal data, you **should** think about why you need it. This will help you to decide whether you will have enough data that is relevant to your story and not more than you actually need.

9.4 You **should** consider any factors people using their data protection rights bring to your attention about how much data you hold.

9.5 You **must** also review the data you hold from time to time (see Keep personal data only for as long as you need to).

Adequate data

9.6 You **must** use enough personal data to do what you need to do, or data that is adequate for your purpose.

9.7 You **must** use accurate personal data, which also involves considering how much data you need (see Use accurate personal data).

9.8 You **should** keep in mind what you are trying to achieve and aim to collect the data that you need to do that efficiently. For example, you **could** plan what questions you need to ask someone in an interview.

Relevant data

9.9 You **must** use personal data that is relevant. Even if personal data is not obviously relevant to a specific story, it can still be relevant to your wider journalistic purpose, but you **should** be able to justify this (see Keep personal data only for as long as you need it).

9.10 Using irrelevant personal data may cause significant harm to people. When using special category or criminal offence data in particular, you **must** only use the data that is relevant (see Use personal data lawfully).

Limited data

9.11 You **must** use personal data in limited ways that are not excessive. For example, you **could** consider the ways you are using personal data throughout the process of developing a story. Although you might have needed to collect a lot of data for background research, you are likely to be more selective about what data to publish.

10. Keep personal data only for as long as you need it

At a glance

- You **must** keep personal data only for as long as you need it.
- There are no specific time limits, so you **should** consider why you are using the data, amongst other factors, to help you decide how long to keep it.
- You **must** act lawfully and fairly when you use the data, so you **should** consider any legal risks and any risk of harm to a person associated with keeping or destroying it.
- Where possible and appropriate, you **must** record how long you expect to hold different types of data.
- You **could** have a retention policy or schedule to help you record standard retention periods, that you could incorporate into your existing processes.
- You **should** review the personal data you hold at appropriate intervals and erase or anonymise any data you no longer need.
- Research and background details, such as contacts, are vital to journalism so it may often be justifiable to keep this data for long periods of time or indefinitely.
- **When the criteria applies, the journalism exemption can remove the usual requirements to:**
  - **keep personal data only for as long as you need it in line with the data protection principle; and**
  - **inform the person concerned when you can demonstrate that the data does not identify them or no longer identifies them (ie it is anonymised and outside the scope of the UK GDPR).**

In more detail

What does keep personal data only as long as you need to mean?

10.1 You **must** keep personal data only as long as you need to. There are no specific time limits so you **should** consider why you are using the data to help you to decide how long it is reasonable for you to keep it.

How do we avoid keeping personal data for longer than we need to?

10.2 How long it is appropriate to keep data for varies depending on the circumstances, however you **must** be able to justify how long you keep it.

10.3 You are in the best position to judge how long to keep personal data to achieve your journalistic purpose. Factors you **could** consider include:

- how likely you are to use the data in the future, taking account of the public interest;
- whether you may need to keep information to defend possible future legal claims;
- any legal or regulatory requirements (eg limitation periods for claims); and
- relevant industry standards or guidelines.

10.4 You **must** also consider the risk of harm to a person if you keep personal data. You **must** only keep personal data if it would be fair and lawful to do so.

10.5 You **must** record how long you expect to hold different types of personal data where possible and review this at appropriate intervals (see Take steps to protect personal data). You **could** use a retention policy or schedule to help you.

10.6 Removing all traces of electronic data is not always possible so you **should** make sure that you put the data beyond use. If it is appropriate to delete data from a live system, you **should** also delete it from any back-up system.

What is the difference between anonymisation and pseudonymisation?

Anonymising personal data means that it is no longer in a form which allows people to be identified – either from that data or by combining it with other data. This means that the data is then outside the scope of the UK GDPR.

Pseudonymisation refers to techniques that replace, remove or transform information that identifies people and keeps that information separate. This is not the same as anonymisation. Data that has been pseudonymised is still personal data covered by data protection law.

Research and background materials

10.7 Research and background details, such as contact details, are vital to journalism, so it may often be justifiable to keep this information for long

periods of time or indefinitely. You are the best judge about what you may need in the future based on your experience.

10.8 However, you **should** still review any data you decide to keep to make sure you still need it. For example, you may no longer need out-of-date contact details.

11. Be clear about roles and responsibilities

At a glance

- If you are dealing with personal data and any third parties, you **should** decide whether they are a controller, joint controller or processor under the UK GDPR. This affects legal responsibilities.
- To decide this, you **should** consider who decides why and how the data is used, known in the UK GDPR as a controller.
- If you ask a third party to help you with a story and they are permitted to act only on your instructions, they are a processor.
- You **must** have a written contract with processors and they must give you sufficient guarantees that they can comply with data protection law.
- If you are acting as a joint controller with a third party this means that you both determine the means and purposes of the using the data. You **must** have a transparent arrangement in place setting out your respective responsibilities.
- When sharing personal data, you **must** keep certain records to comply with the UK GDPR's requirements and carry out a DPIA if there is likely to be a high risk. You **could** also use a data sharing agreement.
- You **must** comply with data protection law if you receive personal data from a third party that you want to use. Relevant checks include confirming the source, how and when the data was collected, and checking its accuracy.
- The specific rules about making international transfers do not apply to online publication.
- **When the criteria applies, the journalism exemption can remove the usual requirements to comply with the general principles for restricted transfers of personal data to countries outside the UK or to international organisations.**

In more detail

What are the possible roles and responsibilities of different parties?

11.1 If you are dealing with personal data and any third parties, you **should** decide whether they are a controller, joint controller or a processor under the UK GDPR. This affects legal responsibilities.

What is the difference between controllers, joint controllers and processors?

The key question is who determines why and how the personal data is used?

Controllers is a term used in the UK GDPR to describe the main decision-makers exercising control over the why and how personal data is used.

If two or more controllers jointly decide why and how the same data is used, they are joint controllers. If the data is being used for different purposes, they are not joint controllers.

Processors act on behalf of, and only on the instructions of, the relevant controller.

How do we make sure that we are clear about roles and responsibilities?

Decide whether a third party is a controller or a processor

11.2 To decide whether a third party is a controller, joint controller or processor, you **should** consider the nature of the activities they are carrying out and how much control they have over why and how data is used.

11.3 For example, private investigators, freelance photographers and journalists are likely, in many cases, to be controllers in their own right. This is because they are likely to have a significant degree of independence to decide for themselves what is the most effective way of doing something, albeit they may still generally act in line with your instructions.

11.4 If acting as a joint controller, you **must** have an agreement with the other party or parties that sets out your respective responsibilities, particularly about transparency and individual rights. You **must** make this information available to people.

11.5 If you ask a third party to help you with a story and they are permitted to act **only** on your instructions, they are a processor, even if they make some technical decisions about how to use the data.

11.6 Whenever you use a processor, you **must** have a written contract with them. You **must** also make sure any processors you use give you sufficient guarantees that they will meet the UK GDPR's requirements and protect people's rights.

Data sharing with third parties

11.7 When sharing personal data between controllers, you **must** comply with the data protection principles. In particular, you **must** share personal data lawfully, fairly and transparently (see Use personal data lawfully, Use personal data fairly and Use personal data transparently).

11.8 You **should** consider our Data sharing code of practice to help you comply with the law and good practice when sharing personal data. This sets out that you **must** keep certain records about the sharing (see Take steps to protect personal data) and you **must** carry out a DPIA if needed (see Take steps to protect personal data).

11.9 You **could** also have a data sharing agreement with other parties to make sure the details are clear, especially if you are sharing data regularly, routinely or it is planned in advance.

Receiving personal data from third parties

11.10 You **must** comply with data protection law if you receive any personal data from another controller that you want to use, such as a freelance journalist or photographer. For example, you **must** make sure you use the data fairly, lawfully, transparently and carry out reasonable accuracy checks (see Use accurate personal data).

International transfers

11.11 The specific rules about making international data transfers do not apply to online publication, even if this makes information available outside the European Economic Union.

12. Help people to use their rights

At a glance

- People have specific data protection rights which they can exercise on request. You **must** help people to use these rights and respond within specific time limits.
- You **can** refuse to comply with individual requests in certain circumstances, including if the request is manifestly unfounded or excessive.
- People can ask for copies of their data. You **should** make reasonable efforts to find relevant information and provide what you can to them.
- There is a very strong, general public interest in protecting the identity of journalists' confidential sources. It is very unlikely you would be required to disclose such information.
- People can also object to your use of their data, ask you to restrict it or erase it in certain circumstances. If you have disclosed the data to others, you **must** tell them if the data is restricted or erased unless this is impossible or involves disproportionate effort.
- The right to erasure does not apply if using the data is necessary to protect the right to freedom of expression and information.
- If data is inaccurate, you **must** correct or complete it. You **should** also consider whether you need to add a note to make sure your records are not misleading.
- There is a strong, general public interest in the preservation of news archives, which contribute significantly to the public's access to information about past events and contemporary history. This is generally a strong factor in favour of not erasing personal data from news archives.
- **When the criteria applies, the journalism exemption can remove the usual requirements to:**
  - **confirm to the person whether you are using their data, provide access to their data as well as other information;**
  - **inform the person when their data is transferred to a country outside the UK or an international organisation;**
  - **provide the person with a copy of their personal data;**
  - **comply with the right to have data completed or corrected, erased, or restricted and the right to object to use of personal data; and**
  - **comply with the right to data portability.**

In more detail

What are individual rights?

12.1 Under data protection law, people have specific rights about their personal data as follows:

- right to be informed;
- right of access;
- right to rectification;
- right to erasure;
- right to object;
- right to data portability; and
- rights related to automated decision-making, including profiling.

12.2 We have focused below on the rights most likely to be relevant to journalism. See Use personal data transparently for information about the right to be informed.

How do we comply with individual rights?

Responding to requests

12.3 People can make requests in writing or verbally to use their rights. There are no specific requirements about how they should do this.

12.4 Generally, you **must** comply with a request without undue delay within one month of receiving it. However, you can extend the time to respond by a further two months, if the request is complex or you have received a number of requests from the person to exercise their data protection rights.

12.5 You **should** have appropriate resources in place to enable you to handle requests and you **should** train staff about what to do if they receive one (See Take steps to protect personal data).

Refusals

12.6 You can refuse to respond to a request if an exemption applies, such as the journalism exemption.

12.7 You can also refuse to comply with a request if it is manifestly unfounded or manifestly excessive. These provisions can help if you receive vexatious or harassing requests.

12.8 You **must** be able to justify any decision you take to refuse someone's request. The key point to consider is whether, objectively, the request would clearly have a disproportionate or unjustifiable impact. This must be obvious because the wording used in the law is "manifestly". Factors you **could** consider include:

- whether the request has any serious purpose or value;
- what is the requester's motive;
- whether the request would impose an unreasonable burden on your resources; and
- if it involves any harassment of your staff.

12.9 An exemption may exempt you in whole or only in part. You **should** avoid taking a blanket approach and consider whether you are able to disclose some of the information, even if some of it is exempt.

12.10 If you refuse to comply with a request you **must** tell the requester:

- why you are refusing the request;
- that there is a right to complain to the ICO or another supervisory authority; and
- there is a right to seek court enforcement.

Right of access

12.11 People have the right to ask you to:

- confirm that you are using their personal data;
- give them a copy of their personal data; and
- provide other supplementary information (often this will already be in a privacy notice which you may have on your website, so you can simply link to it).

12.12 You **should** make reasonable efforts to find relevant information and provide what you can to the requester. You can ask for clarification if you need to.

12.13 You **must not** give someone personal data about another person in response to an access request unless:

- the other person has consented (see Use personal data lawfully); or
- it is reasonable to disclose it without their consent.

12.14 It is very unlikely that you would be required to disclose information about confidential sources in response to a subject access request from another person. In most cases, a confidential source is unlikely to consent to the disclosure of their personal data to a third party. They are also likely to have a strong expectation of confidentiality, which is reflected in the strong

legal protection for journalistic sources. For example, sources are protected under the Contempt of Court Act 1981.

Right to restriction

12.15 People have the right to ask you to restrict the use of their personal data in certain circumstances:

- you have processed their personal data unlawfully and they have requested restriction rather than erasure (see Use personal data lawfully);
- they contest the accuracy of their personal data and you are verifying it (see Use accurate personal data);
- they object to your use of their data and you are considering whether your legitimate reasons override theirs (see Right to object); or
- you no longer need the data but the person concerned needs you to keep it for a legal claim.

12.16 You **must** be able to restrict personal data, if required. You **could** achieve this in different ways, for example:

- temporarily move the data to another system;
- make the data unavailable to users; or
- temporarily remove published data from a website.

12.17 Unless it is impossible or involves disproportionate effort, you must tell each recipient of the data that you have restricted it. If the person concerned wants to know who these recipients are, you **must** tell them.

12.18 In many cases, the restriction is only temporary. You **must** tell the person before you lift the restriction.

Right to rectification (correcting or completing data)

12.19 People have a right to ask you to correct their personal data if it is inaccurate, or to complete it if it is incomplete. This is known as the right to rectification.

12.20 If you receive a request for rectification, you **should** take reasonable steps to check that the data is accurate. Factors you **should** consider include:

- what the requester tells you – they should be able to prove, on the balance of probabilities, that the information is inaccurate;
- any steps you have already taken to verify the accuracy of the personal data (see Use accurate personal data); and
- the risk of harm to the person.

12.21 If appropriate, you **could** restrict your use of the personal data while you check its accuracy even if the person has not specifically requested this.

12.22 If you are satisfied that the data is accurate, you **could** put a note on your internal system recording that the person challenges its accuracy, explaining why.

12.23 If necessary, you **must** correct or complete the data. Even if you took all reasonable steps to make sure the data was accurate at the time, if information later comes to light that suggests it may be inaccurate, you **should** reconsider and take steps to rectify it.

12.24 Opinions are subjective by their nature and not necessarily inaccurate simply because someone disagrees or it is later proven to be incorrect. However, if it becomes clear than an opinion was based on inaccurate data, you **should** correct it.

12.25 If an inaccuracy is only minor, such as a typographical error, it is usually reasonable to simply edit an online article to correct it. However, you **should** consider whether it is appropriate and proportionate to add a note to make sure that your records are not misleading. This may take a variety of forms, for example, an advisory line at the top of an online article, or a printed correction in a newspaper.

12.26 Unless it is impossible or involves disproportionate effort, you **must** tell each recipient that you have rectified the data. If the person concerned wants to know who these recipients are, you **must** tell them.

12.27 If you have published the personal data in multiple locations, such as in print and online, you **should** consider what steps it is reasonable for you to take in each context. For example, on social media platforms, you **could** encourage people who have shared the inaccurate information to help to circulate the correction.

Right to object

12.28 People have the right to object to the use of their personal data if you are relying on the legitimate interests lawful reason for using it (see Use personal data lawfully).

12.29 You **must** clearly tell people about their right to object when you first communicate with them at the latest.

12.30 If someone objects, you **should** consider the reason carefully. However, you may be able to carry on using the data if your legitimate interests in using it are stronger than the person's in the circumstances.

12.31 If you have no reason to refuse the objection, you **must** stop using the personal data. This may mean that you need to erase the personal data, but this is not always appropriate. For example, you may need to retain the data for other purposes.

Right to erasure

12.32 People have the right to have their personal data erased without undue delay if:

- you do not need to keep the personal data for the purpose you originally collected or used it for;
- you are relying on the consent lawful reason, consent is withdrawn and there are no other legal reasons for using the data;
- a person objects to your use of the data (see Right to object) and there are no overriding legitimate reasons for using it;
- you have used personal data unlawfully (See Use personal data lawfully);
- you collected the data to offer online services to a child; or
- you need to erase the data to comply with a legal obligation.

12.33 You **must** give particular weight to any request for erasure if you are using data based on consent given by a child, especially for online services.

12.34 When personal data is made public, you **must** take reasonable steps to inform other parties with legal responsibility for using the personal data about the request. You **must** tell them that the person concerned has asked them to erase any links to the data or any copies or replication of it.

12.35 Unless it proves impossible or involves disproportionate effort, you **must** tell each recipient of the personal data that you have erased it. If the person concerned wants to know who these recipients are, you **must** tell them.

Protection for freedom of expression and information

12.36 Crucially, the right to erasure does **not** apply if using the data is necessary to exercise the right to freedom of expression and information. In practice, this is likely to be similar to balancing public interest considerations proportionately (see Apply the journalism exemption).

12.37 To help you determine whether you need to use the data to exercise the right to freedom of expression, you **should** take into account the factors used by the European Court of Human Rights when balancing these rights.

12.38 These factors are a guide and some may have more or less relevance, depending on the circumstances, including:

- how much the information contributes to a debate of public interest;
- how well known the person concerned is and the subject of the article;
- the prior conduct of the person (eg have they actively invited media attention?);
- how you obtained and verified the information;
- the content, form and impact of the publication; and

- whether the interference with the person's right to privacy is proportionate and justified in light of the above factors.

12.39 An offender may reasonably expect privacy as a result of the passage of time. You **should** take into account the strong public interest in the rehabilitation of offenders (See Use personal data lawfully).

12.40 You **should** take into account that information published online generally poses a higher risk to privacy because of the potential to reach a larger audience than print. This is particularly so when information is amplified by search engines.

News archives

12.41 There is a strong, general public interest in the preservation of news archives, which contribute significantly to the public's access to information about past events and contemporary history. This is generally a strong factor in favour of not erasing personal data from news archives.

12.42 Protecting the integrity of records is vitally important, so any steps considered necessary are unlikely to include erasing or deleting the actual record. For example, you may be required to anonymise a digital archive record so it does not appear in a search using someone's name, leaving the original record as it is and still accessible by less prominent means.